УДК 621.396

ПОТЕНЦИАЛЬНЫЕ ВОЗМОЖНОСТИ ОБНАРУЖЕНИЯ СПЕКТРАЛЬНЫХ СОСТАВЛЯЮЩИХ ПЭМИ СИГНАЛА КЛАВИАТУРЫ USB ИНТЕРФЕЙСА

Соколов Р.И., Астрецов Д.В., Кобяков В.Ю.

*ФГАОУ ВПО Уральский Федеральный Университет имени первого Президента России Б.Н.Ельцина, кафедра радиоэлектронных и телекоммуникационных систем ИРИТ-РТФ, Екатеринбург, Россия (*620002*, Россия, г. Екатеринбург, ул. Мира, 32), e-mail: rostik-king@yandex.ru*

Аннотация: Настоящая статья посвящена исследованию потенциальных возможностей обнаружения информативной и неинформативной составляющих сигнала ПЭМИ клавиатуры USB интерфейса. Проводиться цифровой эксперимент для оценки значения максимума взаимной корреляционной функции спектра сигнала ПЭМИ, снятого с двух информативных проводов, содержащего пакет опроса и ответа с данными и опорного сигнала, в зависимости от отношения сигнал/шум на входе приемного устройства для БГШ и одного из трех видов помех Джонсона с различными параметрами распределения. В результате исследования были установлены потенциальные возможности обнаружения сигнала ПЭМИ клавиатуры интерфейса USB в идеальных условиях без воздействия внешнего шума и в реальных условиях естественного и индустриального шумов. На основании полученных результатов сделан вывод о том, что излучения ПЭМИ клавиатуры интерфейса USB не являются опасными с точки зрения возможного обнаружения в реальных условиях.

Ключевые слова информационная безопасность, побочные электромагнитные излучения, перехват информации, интерфейс USB клавиатуры, защита информации.

POTENTIAL DETECTION SPECTRAL COMPONENT OF COMPROMISING EMANATIONS SIGNAL USB KEYBOARD INTERFACE

R.I. Sokolov, D.V. Astretsov, V.U. Kobyakov

*Institute of Radioelectronics and Informational Technologies, Ural Federal University named after the first President of Russia B.N.Yeltsin, Ekaterinburg, Russia (*620002*, Russia, Ekaterinburg,32 Mira st.), e-mail: rostik-king@yandex.ru*

Abstract: This article is devoted to research potential detection informative and uninformative signal components compromising emanations USB keyboard interface. Digital experiment held to assess the value of the maximum cross-correlation function of the signal spectrum compromising emanations, radiated from two informative wire containing package interrogation and response data and reference signal, depending on the signal / noise ratio at the receiver input for WGN and one of three types of interference Johnson different the parameters of the distribution. As a result, studies have established the potential of the detection signal compromising emanations keyboard USB interface in ideal conditions without the influence of external noise and the actual conditions of natural and industrial noise. Based on the results concluded that the radiation compromising emanations keyboard USB interface are not dangerous from the point of view of a possible encounter in the real conditions.

Key words: safety information, electromagnetic radiation, eavesdropping, USB interface keyboard, compromising emanations.

Качество приёма сигнала побочного электромагнитного излучения зависит от вида излучаемого сигнала, от мощности и от вида распределения помехи. Автоматизированные комплексы для специальных исследований являются универсальными и не рассчитываются для каждого вида сигнала и помехи. Для исследования предельных возможностей перехвата и выработке эффективных средств защиты от перспективных средств разведки, требуется теоретический анализ и моделирование как оптимальных, так и реализуемых на практике алгоритмов настроенных на каждый тип помехи [1].

В открытой печати отсутствует информация о возможности перехвата информационных составляющих спектра сигнала ПЭМИ клавиатуры USB [4]. Предварительный эксперимент показал, что на анализаторе спектра не удается выявить спектральные составляющие, характеризующие информативный сигнал [2,5]. Таким образом, для исследования потенциальных возможностей обнаружения информативной составляющей сигнала ПЭМИ клавиатуры USB и её восстановления требуется проведение эксперимента в режиме широкополосного приема сигнала.

Однако исследования в спектральной области позволяют оценить возможность обнаружения сигнала ПЭМИ клавиатуры интерфейса USB без учета наличия информационных пакетов данных в сигнале. Для того, чтобы оценить потенциальные возможности обнаружения сигнала ПЭМИ клавиатуры интерфейса USB, необходимо определить критические значения отношения С/Ш для различных видов помех (как БГШ, так и индустриальный шум) при которых возможно различение спектров смеси сигнала и шума и шума.

Для этого в ходе цифрового эксперимента 1 оценивается значение максимума взаимной корреляционной функции спектра сигнала ПЭМИ, снятого с двух информативных провода, содержащего пакет опроса и ответа с данными, в зависимости от отношение сигнал/шум на входе приемного устройства для БГШ и одного из трех видов помех Джонсона с различными параметрами γ и η. На рисунке 1 представлена блок схема цифрового эксперимента, а на рисунках 2 представлены результаты эксперимента при отношении С/Ш -5дБ для БГШ. Сигналы ПЭМИ сняты токосъемником ТИ2-3(0,009…300 МГц №0610) и записаны на цифровой осциллограф DPO 2024. В эксперименте 1 одновременно происходит расчет четырех взаимных корреляционных функций. Функция от спектральной маски сигнала ПЭМИ с пакетом запроса и ответа о нажатии клавиши «Q» клавиатуры RAPOO подается на один из входов каждого из четырех корреляторов. На второй вход первого коррелятора подается спектр сигнала с пакетом запроса и ответа о нажатии клавиши «Q» клавиатуры RAPOO (спектр идентичный маске), смешанный с шумом. На второй вход второго коррелятора подается спектр сигнала с пакетом запроса и ответа о нажатии клавиши «Q» клавиатуры RAPOO, снятый в другой момент времени, отличный от спектральной маски, смешанный с шумом. На второй вход третьего коррелятора подается спектр сигнала с пакетом запроса и ответа о нажатии клавиши «Q» клавиатуры Logitech K200, смешанный с шумом. На второй вход четвертого коррелятора подается спектр шума. На рисунках 3 – 6 представлены графики зависимости нормированных значений ВКФ от отношения С/Ш для различных помех. Так же получены зависимости зависимости нормированных значений ВКФ от значений параметров γ и η для S_L, S_B и S_U помех Джонсона.

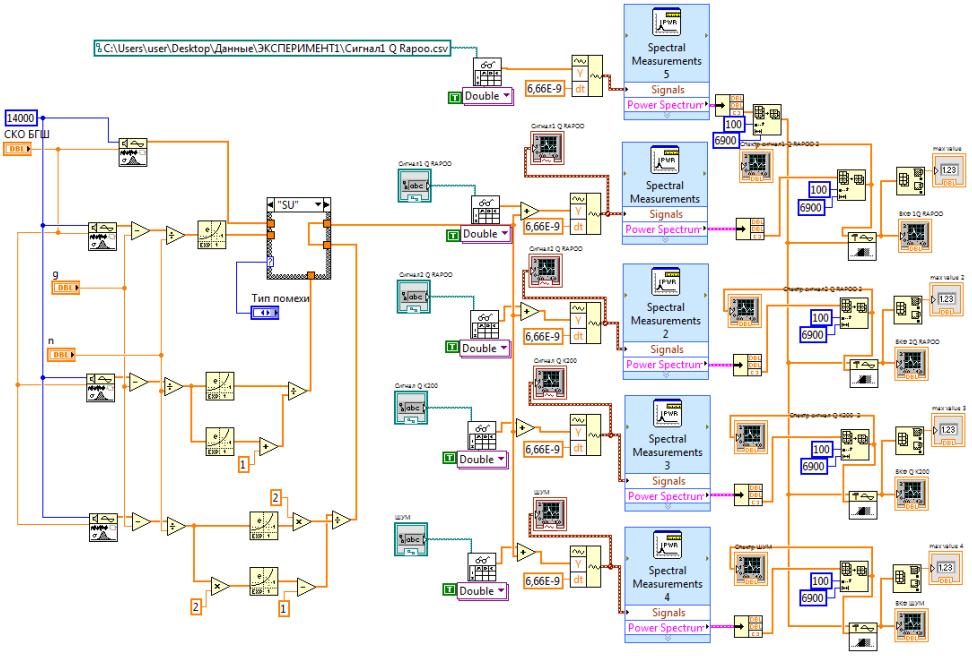

Рис. 1 – Блок схема эксперимента 1.

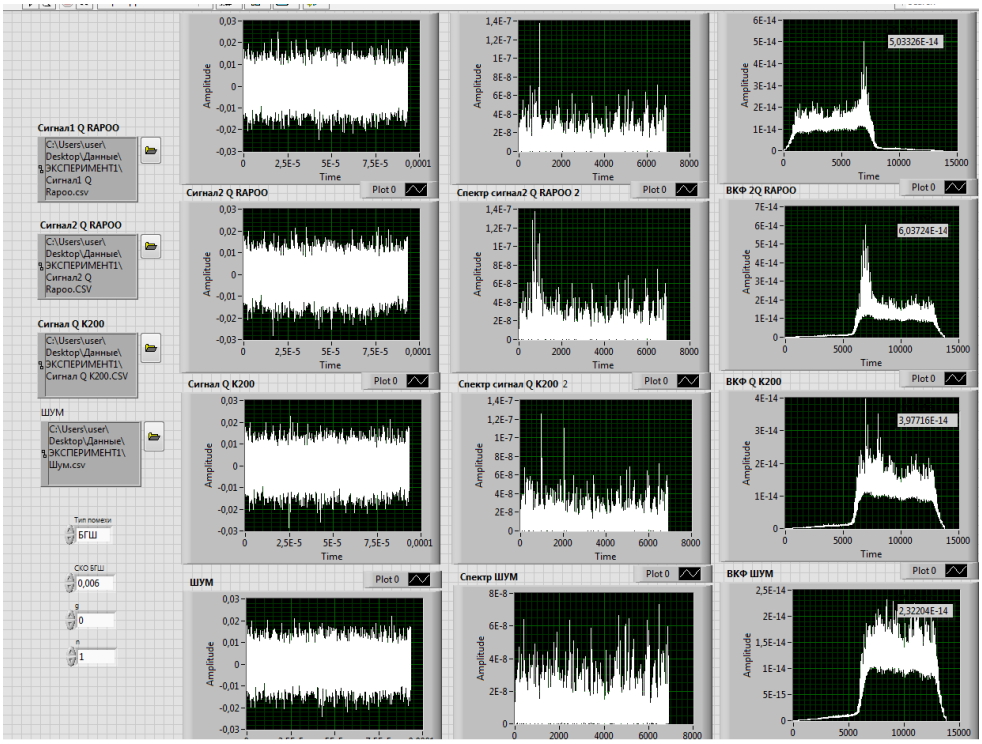

Рис. 2 – Результаты эксперимента 1 при отношении С/Ш -5дБ для БГШ.

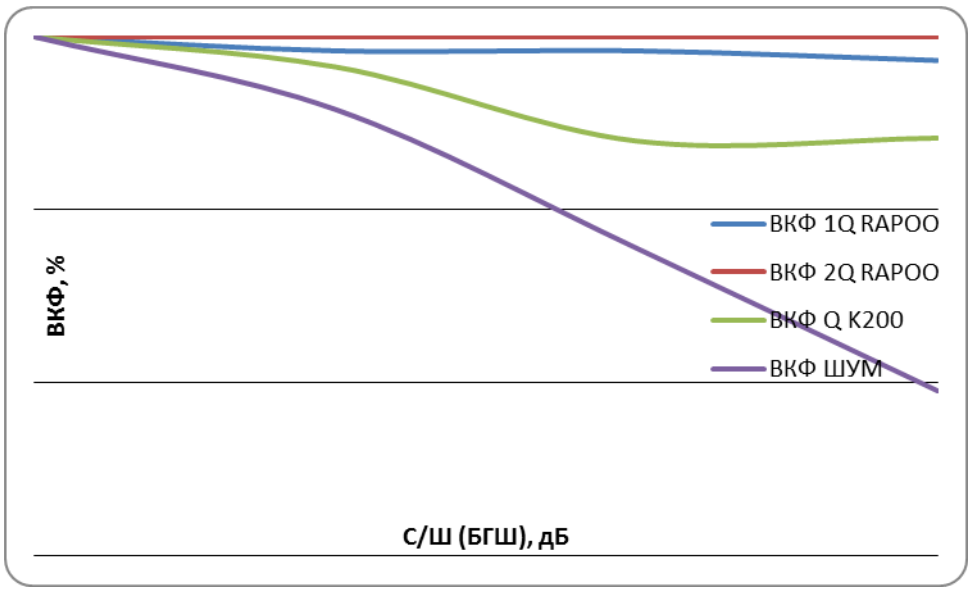

Рис. 3 – График зависимости нормированных значений ВКФ от отношения С/Ш для БГШ.

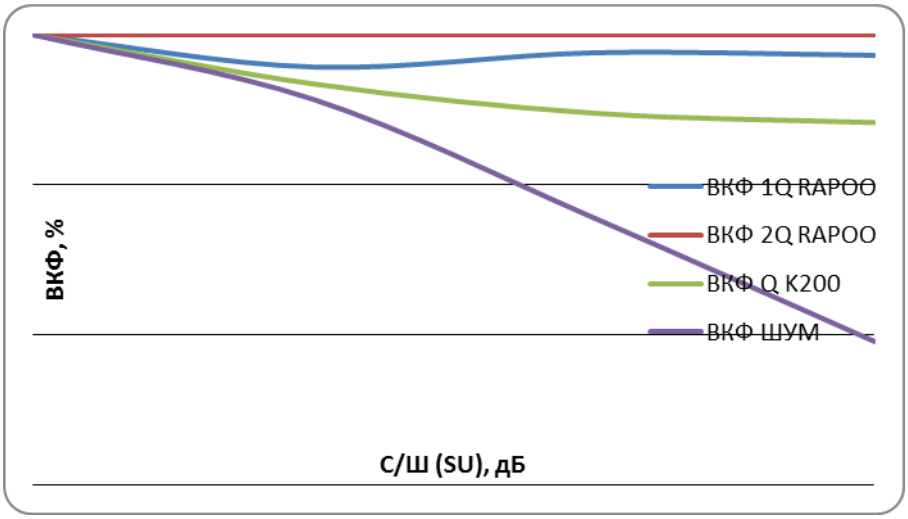

Рис. 4 – График зависимости нормированных значений ВКФ от отношения С/Ш для S_U помехи Джонсона.

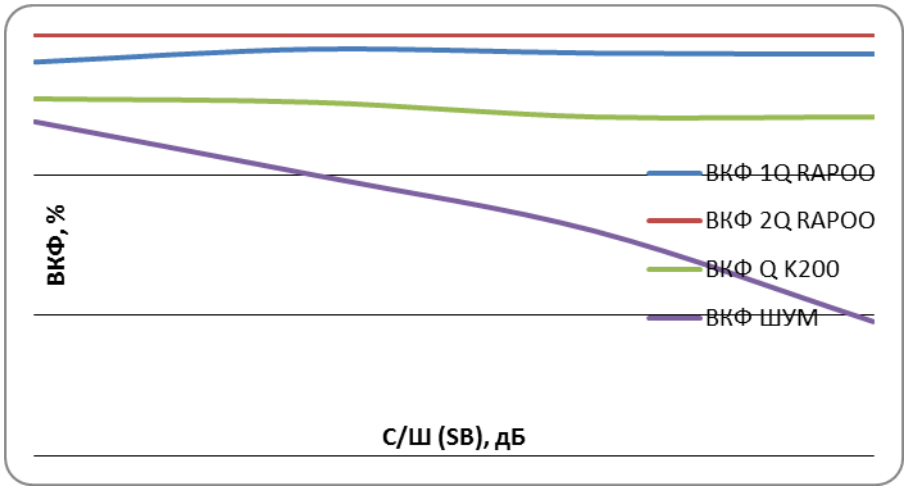

Рис. 5 – График зависимости нормированных значений ВКФ от отношения С/Ш для S_B помехи Джонсона.

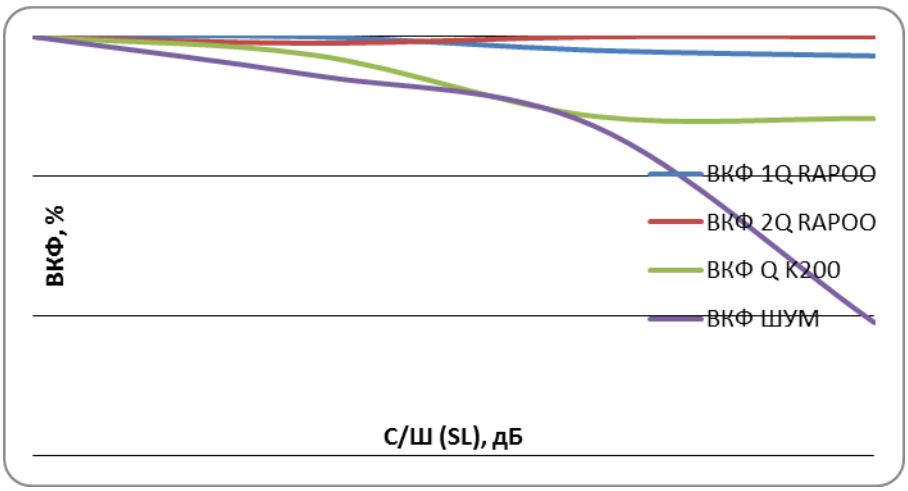

Рис. 6 – График зависимости нормированных значений ВКФ от отношения С/Ш для S_L помехи Джонсона.

На основании полученных данных можно сделать следующие выводы:

1. Для БГШ и S_U помехи Джонсона критическим значением является отношение мощности сигнала к мощности помехи, равное -5 дБ. При этом максимальные значения взаимных корреляционных функций спектра сигнала ПЭМИ и опорной спектральной маски, а также спектра шума без сигнала ПЭМИ и опорной спектральной маски принимают практически не различимые значения.
2. Наихудшим маскирующим эффектом обладает S_B помеха Джонсона, для которой критическим значением является отношение мощности сигнала к мощности помехи, равное -10 дБ. При этом по максимальным значениям взаимных корреляционных функций спектра сигнала ПЭМИ и опорной спектральной маски, снятых с одной клавиатуры, а также спектра шума без сигнала ПЭМИ и опорной спектральной маски возможно обнаружение сигнала с высокой составляющей даже при указанном отношении С/Ш -10 дБ.
3. Наилучшим маскирующим эффектом обладает S_L помеха Джонсона, для которой критическим значением является отношение мощности сигнала к мощности помехи, равное 0 дБ. При этом по максимальным значениям взаимных корреляционных функций спектра сигнала ПЭМИ и опорной спектральной маски, снятых с разных клавиатур, а также спектра шума без сигнала ПЭМИ и опорной спектральной маски практически не возможно обнаружение сигнала даже при указанном отношении С/Ш 0 дБ.
4. Для всех трех видов распределений помех Джонсона увеличение параметра η приводит к снижению маскирующих свойств помехи при заданном уровне мощности помехи. Так, например, для S_L помехи Джонсона увеличение параметра η от 1 до значения 4 приводит к проигрышу в маскирующем действии на 5 дБ.
5. Для всех трех видов распределений помех Джонсона увеличение параметра γ приводит к снижению маскирующих свойств помехи при заданном уровне мощности помехи. Так, например, для S_L помехи Джонсона увеличение параметра γ от 0 до значения 2 приводит к проигрышу в маскирующем действии на 5 дБ.

Для того, чтобы оценить потенциальные возможности обнаружения сигнала ПЭМИ клавиатуры интерфейса USB, необходимо рассчитать:

1. Дальность до точки в пространстве, при которой отношение мощности сигнала к мощности внутренних шумов приемника снизиться до уровня -5 дБ без воздействия внешнего шума.
2. Дальность до точки в пространстве, при которой отношение мощности сигнала к мощности суммы внешних и внутренних шумов приемника снизиться до уровня -5 дБ для БГШ и S_U помехи Джонсона, до -10 дБ для S_B помехи Джонсона, до 0 дБ для S_L помехи Джонсона для стандартизованных параметров распределения (γ=0, η=1).
3. Провести эксперимент 2 по обнаружению спектральных составляющих на расстоянии от излучающего кабеля с помощью анализатора спектра реального времени.
В качестве излучающей модели определим кабель как элементарный электрический вибратор (диполь Герца).
Излученная кабелем мощность определяется интегрированием модуля вектора Пойтинга по всем направлениям $\left(0 \le \theta \le \pi, 0 \le \varphi \le 2\pi\right)$.

$$P_{\Sigma} = 15\pi I_0^2 \left(\frac{l}{\lambda_0}\right)^2 \int_0^{2\pi}\int_0^{\pi} \sin^3\theta \, d\theta d\varphi = 40\pi^2 I_0^2 \left(\frac{l}{\lambda_0}\right)^2 \quad (1)$$

Для расчета излученной мощности P_{Σ} необходимо определить ток, протекающий вдоль кабеля I_0. Из осциллограмм снятых токосъемником, можно определить значение тока I как отношение СКО напряжения U за время пакета и сопротивление нагрузки осциллографа R_o равной 100 Ом. СКО напряжения сигнала с двух информационных проводов 1,5 мВ, с неэкранированного кабеля 0,8 мВ, с экранированного кабеля 0,3 мВ. На частоте 20 МГц, соответствующей полосе сигнала ПЭМИ, коэффициент токосъемника α равен -9дБ. Формула для расчета ток, протекающий вдоль кабеля I_0:

$$I_0\,[\text{дБмА}] = \alpha + 20\,\lg[\text{СКО(U)}/R_o/1\text{мА}] \quad (2)$$

Ток, протекающий вдоль двух информационных проводов -46 дБмА (5 мкА); ток, протекающий вдоль неэкранированного кабеля -51 дБмА (2,8 мкА); ток, протекающий вдоль экранированного кабеля -59 дБмА (1,1 мкА).

Подставляя значения токов I_0 в формулу 1, получаем значения мощностей излученных сигналов ПЭМИ, снятых с кабеля 1 м. При этом необходимо проинтегрировать мощность по частоте в полосе сигнала от 400 кГц до 20 МГц. Общая формула для расчета излучаемой мощности сигнала:

$$P_{\Sigma} = \int_{\lambda 0} 40\pi^2 I_0^2 (l/\lambda_0)^2 = 40\pi^2 I_0^2 (l/\lambda_{01} - l/\lambda_{02}) \quad (3)$$

Мощность, излучаемая сигналом ПЭМИ клавиатуры USB с двух информационных проводов –62 дБм ($6{,}45*10^{-10}$ Вт); мощность, излучаемая сигналом ПЭМИ клавиатуры USB с неэкранированного кабеля -67 дБм ($2*10^{-10}$ Вт); мощность, излучаемая сигналом ПЭМИ клавиатуры USB с экранированного кабеля -75 дБм ($3*10^{-11}$ Вт).

В настоящее время в методиках определения коэффициента реального затухания электромагнитного поля (ЭМП) принимается математическая модель затухания электромагнитного поля в свободном пространстве, в соответствии с которой затухание поля между двумя точками в ближней зоне пропорционально кубу отношения расстояний

между этими точками и источником излучения [3]. На рисунках 7 представлен графики затухания сигнала ПЭМИ с увеличением расстояния до источника.

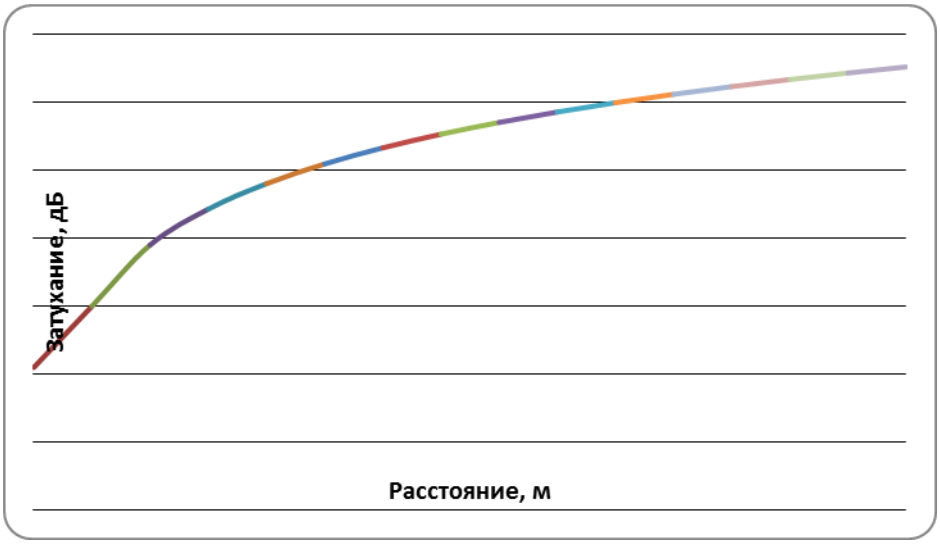

Рис. 7 – График затухания сигнала ПЭМИ от расстояния до источника в ближней зоне.

Таблица 1. Расстояние до источника излучения, на котором возможно обнаружение неинформативного спектра сигнала ПЭМИ клавиатуры интерфейса USB.

Тип помехи	Идеальные условия (отсутствие внешнего шума)			Реальные условия (энергия внешнего шума 10^{-16}Дж)		
	2 провода	4 провода	экран. кабель	2 провода	4 провода	экран. кабель
БГШ	5 м	3 м	2 м	10 см	5 см	<5 см
S_L				5 см	<5 см	<5 см
S_B				15 см	10 см	5 см
S_U				10 см	5 см	<5 см

Мощность внешней помехи в полосе 20 МГц составляет $2*10^{-9}$ Вт, что соответствует -57 дБм. Предельные значения чувствительности анализатора спектра с учетом известных априорных сведениях о распределении помехи: для БГШ и S_U помехи Джонсона -142 дБм, для S_L помехи Джонсона -137 дБм, для S_B помехи Джонсона -147 дБм. Минимальный уровень сигнала на входе анализатора спектра при действии внешних помех: для БГШ и S_U помехи Джонсона -85 дБм, для S_L помехи Джонсона -80 дБм, для S_B помехи Джонсона -90 дБм. Максимальное ослабление сигнала ПЭМИ, излучаемое экранированным кабелем, при действии внешних помех для обнаружения характерных спектральных составляющих определяется как разница между предельным значением чувствительности анализатора и суммой мощностей излученного сигнала и внешней помехи: для БГШ и S_U помехи Джонсона 10 дБ, для S_L помехи Джонсона 5 дБ, для S_B помехи Джонсона 15 дБ.

Максимальное ослабление сигнала ПЭМИ, излучаемое экранированным кабелем, в отсутствии внешних помех для обнаружения характерных спектральных составляющих 67 дБ.

Из графика на рисунке 7 и максимально допустимых рассчитанных значений затуханий определяются предельные расстояния обнаружения ПЭМИ сигнала клавиатуры интерфейса USB для идеальных и реальных условий, представленные в таблице 1.

Полученные расчетные данные для реальных условий подтверждаются натуральным экспериментом. На рисунках 8 и 9 представлены спектры сигнала ПЭМИ клавиатуры RAPOO, снятые широкополосной магнитной антенной АИР 3-2 на расстоянии 10 см от неэкранированного и экранированного кабеля.

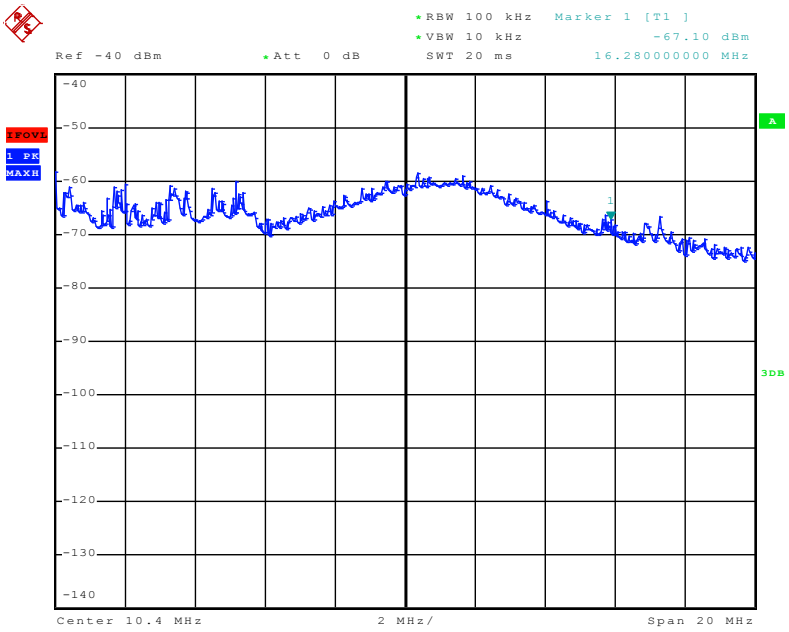

Рис. 8 – Спектр сигнала ПЭМИ клавиатуры USB, снятый с неэкранированного кабеля на расстоянии 10 см.

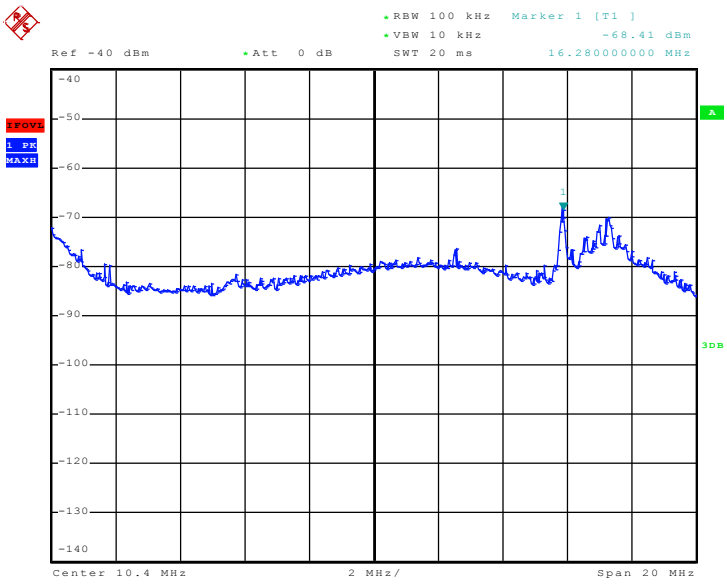

Рис. 9 – Спектр сигнала ПЭМИ клавиатуры USB, снятый с экранированного кабеля на расстоянии 10 см.

На спектре сигнала, снятого с четырех проводов на расстоянии 10 см отчетливо видны спектральные составляющие сигнала ПЭМИ. На расстоянии 10 см с экранированного кабеля предельно различимо наблюдаются отдельные частотные составляющие спектра сигнала ПЭМИ.

В результате исследования были установлены:

1. Потенциальные возможности обнаружения сигнала ПЭМИ клавиатуры интерфейса USB в идеальных условиях без воздействия внешнего шума. При этом дальность обнаружения составила около 2 м от экранированного кабеля.
2. Реальные возможности обнаружения сигнала ПЭМИ клавиатуры интерфейса USB в условиях естественного шума БГШ. При этом дальность обнаружения не превышает 5 см от экранированного кабеля для БГШ и S_U , S_L и S_B помехи Джонсона. Таким образом, можно сделать вывод о том, что излучения ПЭМИ клавиатуры интерфейса USB не являются опасными с точки зрения возможного обнаружения в реальных условиях.
3. В результате цифрового моделирования и натурного эксперимента не удалось обнаружить информационные спектральные составляющие сигнала ПЭМИ. Таким образом, спектральный анализ позволяет определить наличие излучения, то есть позволяет оценить только возможности обнаружения сигнала, и не позволяет оценить возможности восстановления.
4. Для оценки возможностей восстановления сигнала требуется проведение специальных исследований в режиме приема и обработки сигналов во времени.

Список литературы

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т.1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. - 436 с.
2. Кобяков В.Ю., Лучинин А.С. ОБНАРУЖЕНИЕ ПЭМИ ПРОВОДНИКОВ И КОННЕКТОРОВ ПРИ ПЕРЕДАЧЕ ПО ИНТЕРФЕЙСУ USB. Вестник УрФО. Безопасность в информационной сфере. №14, 2014 г., с 4-8.
3. Фролов В.Ю. Расчет коэффициента стандартного затухания эм-поля на основе модели затухания эм-поля в свободном пространстве / В. Ю. Фролов, А. А. Погорелов, В. В. Петров / Информационно-методический журнал «Inside. Защита информации», №3 – 2005 г.
4. Martin Vuagnoux, Sylvain Pasini. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards, EPFL, Lausanne, Switzerland. http-www. usenix.org-events-sec09-tech-f ull_papers-vuagnoux. pdf
5. USB Hid Keyboard Scan Codes www.mindrunway.ru/.../USBKeyScan.pdf

References

1. Horev A. A. Technical protection of information: textbook. textbook for University students. In 3 T. T. 1. Technical channels of information leakage. M.: SPC "Analyst", 2008. - 436 p.
2. Kobyakov, V. Yu., Luchinin A. S. DETECTION of TEMPEST CONDUCTORS AND CONNECTORS WHEN TRANSFERRING VIA USB. Urfr Newsletter. Security in the information sphere. No. 14, 2014, from 4-8.
3. Frolov, V. Y. Calculation of a standard coefficient of attenuation of the em field model-based attenuation of the em field in free space / V. Y. Frolov, A. A. Pogorelov, V. V. Petrov / Informational-methodological journal "Inside. Information protection", No. 3 – 2005
4. Martin Vuagnoux, Sylvain Pasini. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards, EPFL, Lausanne, Switzerland. http-www. usenix.org-events-sec09-tech-f ull_papers-vuagnoux. pdf
5. USB Hid Keyboard Scan Codes www.mindrunway.ru/.../USBKeyScan.pdf